AF/IFW

Attorney Docket No. 4414-35

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Patent Application

I hereby certify that this paper is being deposited on this date with the U.S. Postal Service as first class mail addressed to Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

Signature Lisa M. Hanlin Date: June 5, 2006

Applicant(s): A. Juels
Case: 4414-35
Serial No.: 10/782,309
Filing Date: February 19, 2004
Group: 2635
Examiner: William L. Bangachon

Title: Low-Complexity Cryptographic Techniques for use with Radio Frequency Identification Devices

---

TRANSMITTAL OF REPLY BRIEF

Mails Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

Submitted herewith is the following document relating to the above-identified patent application:

(1) Reply Brief.

It is believed that there is no additional fee due in conjunction with the response. In the event of any non-payment or improper payment of a required fee, the Commissioner is hereby authorized to charge or to credit **Ryan, Mason & Lewis, LLP Account No. 50-0762** as required to correct the error.

Respectfully submitted,

Joseph B. Ryan

Date: June 5, 2006

Joseph B. Ryan
Attorney for Applicant(s)
Reg. No. 37,922
Ryan, Mason & Lewis, LLP
90 Forest Avenue
Locust Valley, NY 11560
(516) 759-7517

Attorney Docket No. 4414-35

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Patent Application

Applicant(s): A. Juels
Case: 4414-35
Serial No.: 10/782,309
Filing Date: February 19, 2004
Group: 2635
Examiner: William L. Bangachon

I hereby certify that this paper is being deposited on this date with the U.S. Postal Service as first class mail addressed to Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

Signature Lisa M. Hamlin Date: June 5, 2006

Title: Low-Complexity Cryptographic Techniques for use with Radio Frequency Identification Devices

---

REPLY BRIEF

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

The remarks which follow are submitted in response to the Examiner's Answer dated April 5, 2006 in the above-identified application. The arguments presented by Applicant (hereinafter "Appellant") in the Appeal Brief dated January 9, 2006 are hereby incorporated by reference herein.

Appellant initially notes that, responsive to the Appeal Brief, the Examiner has withdrawn the §103(a) rejection of dependent claims 8 and 28. See the Answer at page 2, last paragraph, to page 3, first paragraph. Accordingly, these claims are no longer part of the appeal. Claims 8, 17-19, 21, 22 and 28 are indicated as containing allowable subject matter, and claims 1-7, 9-16, 20, 23-27 and 29-33 are appealed.

Appellant will respond herein to certain arguments raised by the Examiner in Section 6, pages 11-19, of the Answer. Page number references are to the Answer unless otherwise indicated.

At page 11, second paragraph, to page 12, first paragraph, the Examiner argues with regard to independent claim 1 that it would be obvious to apply the teachings of Dannhaeuser to those of Hughes because Hughes is "concerned with communication security" and the Dannhaeuser reference is directed to "foiling attempts of code grabbers." The problem with this argument is that the Examiner relies on the secret key value 66 of Hughes as allegedly meeting the claimed pseudonym. However, this secret key value is clearly a secret that is shared between one or more of the RFID tags 44 and the reader 32, and as such should not be transmitted over "a public, open channel." See Hughes at column 5, lines 46-50, column 6, lines 7-11, and column 8, lines 7-8. If the secret key value 66 of Hughes were to be transmitted, as proposed by the Examiner, there would be no security whatsoever in the Hughes system. Hughes does not teach to transmit this secret key value, and to the contrary specifically teaches to store it as a shared secret between the RFID tag(s) and the reader. Accordingly, it is respectfully submitted that one skilled in the art would not consider transmitting the secret key value 66 itself from the RFID tag 44 to the reader 32 in the Hughes system.

The fact that Hughes is "concerned with communication security" as stated by the Examiner indicates that the secret key value should not be transmitted at all, and instead a complex authentication protocol should be carried out between RFID tag and reader based on their shared secret, as described in FIG. 3 and column 6, lines 7-52, of Hughes. This is not motivation for the proposed combination with Dannhaeuser. To the contrary, it is a direct teaching away from the proposed combination, since Dannhaeuser teaches to sequence through codes that are actually transmitted from transmitter 1 to receiver 2 of FIG. 1 therein over a public, open channel. See Dannhaeuser at column 2, line 60, to column 3, line 24. Since the secret key value 66 in Hughes is not to be transmitted at all, but is instead maintained as a closely-guarded secret essential to the security of the Hughes system, one skilled in the art would not be motivated to apply the code sequencing of Dannhaeuser to the secret key value 66 in the Hughes system.

Even if one assumes for purposes of argument that the secret key value 66 comprises a pseudonym as recited in claim 1, capable of uniquely identifying a given RFID tag, this value is nonetheless a secret key that clearly is not transmitted from the RFID tag 44 to reader 32, and Hughes in fact teaches that it should not be so transmitted. See Hughes at column 5, lines 45-50. Thus, even if secret key value 66 is used to identify a particular RFID tag in conjunction with the

complex authentication protocol of FIG. 3 in Hughes, it nonetheless remains a secret shared between the RFID tag and the reader, forming the basis for the security of the Hughes system, and accordingly should not be transmitted. The foregoing non-obviousness argument is therefore consistent with the definition of pseudonym which Appellant provided at page 5, lines 20-23, of the specification. Again, Dannhaeuser teaches to apply a sequencing technique to codes that are actually transmitted between a transmitter and a receiver. Since the secret key value 66 is not and should not be so transmitted, one would not consider it a candidate for the Dannhaeuser code sequencing approach, absent some explicit teaching or suggestion to do so. Accordingly, it appears that the Examiner has used the present specification as a blueprint to reconstruct claim 1 from disparate references.

At page 13, first full paragraph, the Examiner argues that certain arguments in the Appeal Brief, identified as point (a) and (b), go beyond the claim limitations. Appellant respectfully disagrees.

With regard to point (a), Appellant is simply pointing out the well-known fact that that a common type of conventional RFID device "will typically broadcast its unique identifying information to any nearby reader." See the specification at page 2, lines 3-9. Appellant is not arguing that this particular language is a part of any claim. Instead, it is brought up simply to indicate that Hughes appears to be a conventional system of this type, wherein a code identifier is transmitted from an RFID tag 44 to reader 32 as shown at 40 in FIG. 2 of Hughes. See Hughes at column 5, lines 7-8.

With regard to point (b), Appellant is simply relying on the well-known meaning of the term "one-time pad" in the art of cryptography, in a manner that is consistent with usage of the term in the specification. Since the term "one-time pad" is actually present in the claim at issue, namely claim 33, and is supported by the specification at page 10, lines 11-17, Appellant is not arguing terms not present in the claim.

At page 13, last paragraph, to page 14, first paragraph, the Examiner argues that page 8 of the present specification "states that pseudonyms, by way of example, are 'seeds, secrets, hashes or other information . . . used to generate the pseudonyms'" and so the secret key values 66 of Hughes can be pseudonyms as claimed. Appellant believes that the Examiner is misinterpreting the relied-upon portion of the specification. As indicated previously, the specification at page 5,

lines 20-23, provides a definition of the term pseudonym. The portion of the specification relied on by the Examiner, at page 8, lines 15-21, provides as follows:

> An authorized verifier is able to determine that the different transmitted pseudonyms are associated with the same RFID device. By way of example, such a verifier may have possession of (i) the pseudonyms themselves; (ii) seeds, secrets or other information used to generate the pseudonyms; or (iii) hashes of the pseudonyms or other information generated from the pseudonyms. A verifier of the transmitted pseudonyms must have possession of such information in order to be able to determine that each of the transmitted pseudonyms is associated with the same tag.

The above passage does not state, for example, that the pseudonyms themselves in the corresponding illustrative embodiment are secrets, as alleged by the Examiner, but simply indicates that secrets used to generate the pseudonyms in that embodiment may be in the possession of a verifier. Accordingly, it is believed that the argument proffered by the Examiner on this point misinterprets the above passage from the specification.

At page 14, first paragraph, the Examiner apparently argues that the secret key values 66 are pseudonyms because an RFID device must transmit identifying information. Obviously, an RFID device must transmit identifying information to serve its function within an RFID system. However, as was noted above, an RFID system such as that disclosed in Hughes would not be configured to transmit the very information upon which the security of the system is based, namely a shared secret key used in a complex authentication protocol. Appellant does not dispute that the RFID tags 44 in Hughes transmit an identification code to the reader 32 as part of signal 40, as indicated at column 5, lines 7-8, of Hughes. What Appellant is arguing is that Hughes does not teach or suggest the transmission of the secret key value 66 over a public, open channel, such as that typically present between a reader and an RFID device in an RFID system. Thus, as was pointed out previously herein, even if one assumes for purposes of argument that the secret key value 66 is a pseudonym for a particular RFID tag 44, that secret key value will not be transmitted. Claim 1 calls for transmission of a pseudonym from an RFID tag to a reader, with an authorized verifier able to determine that various received pseudonyms are associated with the same RFID device.

At page 14, bottom half of the page, the Examiner argues that the system of Hughes does not teach away from the claimed invention because Hughes teaches that an RFID tag responds to

a reader query with device-identifying information. Again, this is consistent with the conventional operation of an RFID system as described by Appellant at, for example, page 1, lines 19-21, of the specification. Appellant is arguing that the Hughes system teaches away from the claimed invention as set forth in claim 1, for example, because it teaches to transmit conventional identifiers in response to reader queries, as recited in column 5, lines 7-8, of Hughes. The Examiner is arguing that the secret key value 66 of Hughes may be a pseudonym for a given RFID tag 44, but even if one accepts this premise for purposes of argument, such a secret key value is not transmitted in Hughes. Hughes instead indicates that the security of the system disclosed therein depends on keeping that secret key value 66 as a secret known by only the reader and tag(s), and thus teaches that the secret key value should not be transmitted over a public, open channel. This is a teaching away from, for example, claim 1, which calls for transmission of different pseudonyms in response to different reader queries of the same RFID device.

At page 15, first paragraph, the Examiner apparently disputes that the proposed combination of Hughes and Dannhaeuser would be undesirable or unworkable in an RFID system. The combination proposed by the Examiner is apparently to rotate the secret key values 66 in Hughes using the technique described in Dannhaeuser. As Appellant has argued, such an arrangement would not be appropriate, because Hughes indicates that the secret key values 66 should not be transmitted, and accordingly it would be wasteful of resources to rotate such values using the Dannhaeuser technique. Dannhaeuser sequences through the codes because the codes themselves are actually transmitted over a public, open channel. Since the Hughes secret key values 66 should not be transmitted over such a channel, there would not appear to be any need to rotate them in a manner such as that implemented by Dannhaeuser. Also, as Appellant has pointed out, there are practical considerations. Rotating secret key values 66 in each of the many tags of a typical instance of the Hughes RFID system would place considerable computational burdens on both the tags and the readers, undermining the utility of the system. See Hughes at column 5, lines 8-9, and column 6, lines 3-6.

At page 15, second paragraph, the Examiner argues that Appellant is attacking references individually. Appellant respectfully disagrees. The arguments objected to by the Examiner relate to the lack of motivation to combine Hughes with Dannhaeuser. In arguing lack of

motivation, Appellant has simply described certain aspects of the individual references that are incompatible with one another.

At page 15, last paragraph, to page 16, first paragraph, the Examiner makes reference to the teachings at column 7, lines 48-58, of Hughes, relating to use of public key cryptography. However, in public key cryptographic implementations of Hughes, the private key of the RFID tag takes the place of the secret key value 66, but is nonetheless a secret value that should not be transmitted. Accordingly, these portions of Hughes fail to overcome the deficiencies of the primary embodiment described therein as applied to claim 1.

At page 16, second paragraph, the Examiner argues that the obviousness reasoning is not based on improper hindsight. However, the Examiner argues that one skilled in the art would be motivated to apply Dannhaeuser code rotation to secret key values maintained in the Hughes RFID tags and readers. Where exactly is the suggestion to rotate these secret key values? Certainly not in Hughes, which teaches that the secret key values should not be transmitted over a public, open channel and accordingly would not need frequent rotation of the type described in Dannhaeuser. Dannhaeuser does not provide the motivation, since it teaches to rotate transmitted keyless entry codes which are transmitted over a public, open channel. The only reasonable conclusion is that the suggestion came from the disclosure provided by the present specification.

At page 16, last paragraph, to page 17, first paragraph, the Examiner argues that the fact that the Dannhaeuser technique has been known for many years and yet not applied to conventional RFID systems "is moot since Hughes is the primary reference." Hughes discloses nothing more than an otherwise conventional RFID system, of a type known for many years, augmented by a complex authentication protocol. See the specification at page 1, lines 19-21. If the claimed arrangements were indeed obvious, why has no skilled artisan heretofore thought to apply code rotation from the remote keyless entry context to identifiers in the RFID context? One reason, proffered by Appellant, is that it would in fact not be obvious to do so.

At page 17, second paragraph, the Examiner states that claims 5, 6, 20 and 25-29 recite mathematical formulas that amount to abstract ideas. Appellant initially notes that claim 28 has been indicated as containing allowable subject matter elsewhere in the Answer. With regard to the other claims, the mere presence of mathematical notation is not sufficient ground on which to base a rejection of any claim. The proposed combination of Hughes and Dannhaeuser simply

fails to meet the limitations of these claims. The claims do not recite "abstract ideas that can be practiced by the random number generator or the code sequencing of Dannhaeuser" as is specifically alleged. In the Appeal Brief, Appellant pointed out the particular portions of these references relied on by the Examiner, and argued that those portions failed to meet the claim limitations at issue.

At page 17, last paragraph, the Examiner states that the arguments provided in the Appeal Brief with regard to dependent claims 2-4, 7-16, 23 and 24 amount to a general allegation. Appellant respectfully disagrees. First, claim 8 is indicated as containing allowable subject manner elsewhere in the Answer. Also, for each claim for which separate patentability is argued, the claim is separately described, the portions of the cited references relied upon by the Examiner are presented, and an argument is made that the relied-upon portions fail to meet the claim limitations in question. Accordingly, the proffered arguments as to the claims for which separate patentability is argued are believed to be appropriate. Claims not separately argued stand or fall with other claims, as is entirely appropriate.

At page 18, first paragraph, the Examiner argues that the Appellant has made certain admissions regarding claim scope. Appellant respectfully disagrees with this characterization of his previous arguments, and has made no such admissions. For example, Appellant does not and has not admitted that "the limitations of claims 1 and 3 are a lot narrower than the limitations of claim 33" as alleged.

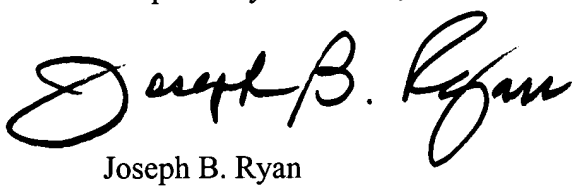
At page 18, last paragraph, to page 19, first paragraph, the Examiner takes exception with certain deficiencies that Appellant has repeatedly noted in the stated rejections. For example, the Examiner has indicated that claim 31 recites the combination of claims 1 and 3, which is clearly incorrect. The error was brought to the attention of the Examiner, and the Examiner apparently has declined to acknowledge or correct the error. See the Appeal Brief at page 11, in the section dealing with claim 31. A similar situation exists with regard to claim 33. See the Appeal Brief at page 10, in the section dealing with claim 33.

The other points raised by the Examiner in the final portion of the Answer have been addressed elsewhere herein. For example, the Examiner again argues that page 8 of the specification states that pseudonyms in the corresponding illustrative embodiment may comprise secrets such as shared secret key value 66 of Hughes. As noted above, the relied-upon passage at page 8, lines 15-21, does not state that the pseudonyms themselves in the illustrative embodiment

may be secrets, as alleged by the Examiner, but simply indicates that secrets used to generate the pseudonyms in that embodiment may be in the possession of a verifier. This appears to be a clear misinterpretation of the actual language from the specification.

For the reasons identified above and in the Appeal Brief, Appellant respectfully submits that claims 1-7, 9-16, 20, 23-27 and 29-33 are in condition for allowance, and respectfully requests the withdrawal of the §103(a) rejections.

Respectfully submitted,



Date: June 5, 2006

Joseph B. Ryan
Attorney for Appellant(s)
Reg. No. 37,922
Ryan, Mason & Lewis, LLP
90 Forest Avenue
Locust Valley, NY 11560
(516) 759-7517